

Amendment Dated July 10, 2008
Serial No. 09/740,052

REMARKS

Reconsideration of the rejection of the claims in this application is respectfully requested. By this amendment, claims 3 and 12 have been canceled, and claims 1, 7, 10, and 16 have been amended. Currently, claims 1, 4-10, and 13-18 are pending in this application.

Rejection of claims under 35 USC 103 over Ma in view of Staples

Claims 1, 3-10, and 12-18 were rejected under USC 103 over Ma (U.S. Patent No. 5,953,338) in view of Staples et al (U.S. Patent Application Publication No. 2002/0118671). This rejection is respectfully traversed in view of the amendments to the claims and the following arguments.

A local area network may be implemented using links with relatively high bandwidth. The network may be connected to an access link, such as provided by an ISP, that may have a much lower bandwidth. For example, in the application applicants give the example of a 10/100 Mbits/sec Ethernet network connected to a 1.5Mbit/sec T1 Internet connection. (Specification at page 4, lines 11 to 15). Where a VPN server is deployed behind the edge of the network, the VPN server will encrypt traffic to be transmitted out of a gateway such as a router connected between the high speed connections of the Local Area Network and the lower speed connection to the Internet. This presents a problem in that the VPN server is not connected to the lower speed link and, accordingly, isn't aware of congestion on the lower speed link. By contrast, the gateway/router knows of the contention but can't intelligently decide which packets should be dropped since the packets have been encrypted by the VPN server.

Applicants proposed to resolve this dilemma by enabling the VPN server to meter traffic belonging to different application groups to enable the VPN server to manage the bandwidth of the access link even though it wasn't connected to the access link. None of the references, alone or in combination, teach or suggest using a VPN server in this manner.

Ma teaches a centralized control module 160 that communicates with ATM edge switches 130 to establish ATM virtual connections through the ATM network. The call control module has a call control module 140, a centralized call admission control/usage monitor 145, and a bandwidth manager module 150. The call control module directly and indirectly controls the operation of the ATM switches to enable a centralized network-wide call admission strategy

Amendment Dated July 10, 2008
Serial No. 09/740,052

to be implemented and to allow connections to be set up on the network. (Mat at col. 8, lines 41-46 and at Col. 7, lines 1-8)

The Examiner has contended that it would have been obvious to include VPN processes in the server 160. Applicants have repeatedly traversed this position. The server 160 in Ma is a centralized controller that is controlling how connections are established on the network. It isn't handling packets on the connections. That is performed by the ATM switches. Once the server establishes the connection, it is not involved in handling packets on the connections. Accordingly, applicants respectfully submit that it would not have been obvious to cause the centralized call controller, which is designed to implement a network-wide call admission control, to perform VPN functions such as encrypting packets on the connections, etc.

In Ma, there are two aspects to the network. The first is a control aspect, which is being implemented by the server 160. The second is the data aspect, which is being handled by the ATM switches 130. The control plane implemented by the server 160 decides which connections should be implemented. It then instructs the data plane, implemented by the ATM switches 130, to cause the connections to actually be set up. The ATM switches then handle the data on the connections independent of the control server 160.

The VPN functions that are recited in independent claim 1 are data functions. That is why claim 1 was amended previously to recite that the VPN server performs the functions of authenticating and/or encapsulating at least a portion of the packets belonging to the application group. Applicants do not understand why it would be obvious for the control server 160, which implements the control plane on the ATM network of Ma, to perform the data plane functions of authenticating and/or encapsulating packets. Accordingly, applicants respectfully traverse the rejection of claim 1 and those claims dependent thereon, and respectfully request that the rejection be withdrawn.

The Examiner cited Staples as disclosing a data communication system comprising a VPN server 122. Applicants concede that Staples shows a VPN server and admitted in the background section of this application that VPN servers were known. (See specification at page 1, lines 5-21). Thus, applicants are prepared to concede that VPN servers were known to exist at the time the application was filed.

Applicants contention is that VPN servers, at that time, did not filter packets belonging to application groups to reduce contention on remote links. The VPN server in Staples does not

Amendment Dated July 10, 2008
Serial No. 09/740,052

appear to do this, and the Examiner has not cited any other reference that performed this function.

The Examiner's main contention appears to be that, since it was known to use a network controller to establish virtual circuits in an ATM network, that it would therefore be obvious to include the functions of the VPN server into the network controller. Applicants respectfully traverse this assertion, since a person skilled in the art would not look to implement VPN functions, which are data plane functions, in the network control system. Accordingly, applicants respectfully request that the rejection be withdrawn.

To facilitate prosecution of this case, applicants have amended independent claim 1 to recite that the Virtual Private Network (VPN) server is connected to links on a network and handles packets of data on the network that will flow over a remote link not connected to the VPN server and that the VPN server manages bandwidth of the remote link. Specifically, applicants have amended claim 1 to recite that the remote link "has a smaller bandwidth than a bandwidth of the links on the network that are connected to the VPN server," and that "the remote link is remote from the VPN server such that the remote link is not directly connected to the VPN server."

A limitation similar to this, albeit differently worded, was previously set forth in dependent claim 3. Accordingly, that claim has been canceled. In connection with claim 3, the Examiner stated that Ma teaches a server that is directly connected to other links (302) having a larger bandwidth than the available bandwidth of the remote links (310-316). The amendment to claim 1 clarifies that the remote links are not directly connected to the VPN server. The links 310-316 which the Examiner cited as examples of "remote links" are clearly directly connected to the ATM edge switch shown in Fig. 3 of Ma. Accordingly, this amendment distinguishes that aspect of Ma as well.

Similar amendments have been made to independent claim 10. Accordingly, that claim is similarly believed patentable over the combination of Ma and Staples.

Conclusion

Applicants cordially invite the Examiner to call the applicants to discuss this case if the Examiner feels that discussing the case may be helpful in any way, or if it appears to the Examiner that the amended claims still fail to overcome the art of record. Likewise, if the

Amendment Dated July 10, 2008
Serial No. 09/740,052

If the Examiner has any questions regarding the amendments or these remarks, the Examiner is requested to telephone the undersigned at the telephone number listed below.

If any fees are due in connection with this filing, the Commissioner is hereby authorized to charge payment of the fees associated with this communication or credit any overpayment to Deposit Account No. 502246 (Ref: NN-13361).

Respectfully Submitted



John C. Gorecki
Registration No. 38,471

Dated: July 10, 2008

Anderson Gorecki & Manaras LLP
P.O. Box 553
Carlisle, MA 01741
Tel: (978) 264-4001
Fax: (978) 264-9119